Lorraine E. Walden

09/10/04

CLMSPTO

Please cancel claims 1 thru 28, and add claims 29 thru 32.

What is claimed is:

1. A production protection system dealing with contents that are digital production, comprising:

obtaining means for obtaining data including at least one of a first content, on which first encryption has been performed and a second content, on which second encryption has been performed, the second encryption is more difficult to break than the first encryption;

first content decryption means for decrypting the first content using a first decryption method that corresponds to the first encryption when the data that has been obtained by the obtaining means includes the first content; and

second content decryption means for decrypting the second content using a second decryption method that corresponds to the second encryption and is more difficult than the first decryption method when the data that has been obtained by the obtaining means includes the second

content.

2. The production protection system according to Claim 1, wherein

the obtaining means and the first content decryption means are realized by a personal computer that executes software for decrypting contents, and

the second content decryption means is realized by one of tamperproof hardware and an apparatus that executes tamperproof software.

3. The production protection system according to Claim 2, wherein the obtaining means obtains the data by receiving the data from an outside network,

the production protection system, further comprising:

replay means for audio-visually replaying the first content that has been decrypted by the first content decryption means;

encryption means for performing third encryption, which is different from the second encryption, on the second content that has been decrypted by the second content decryption means; and

recording means for recording at least part of the second content on which the third encryption has been performed by the encryption means on a recording medium.

4. The production protection system according to Claim 3, wherein the encryption means and a data communication channel between the second content decryption means and the encryption means are realized by one of tamperproof hardware and an apparatus that executes tamperproof software.

5. The production protection system according to Claim 3, wherein an encryption algorithm that is used by the second content decryption means partially differs from an encryption algorithm that is used for encryption by the encryption means.

6. The production protection system according to Claim 3, further comprising:

PC connecting means for connecting to the personal computer via a predetermined interface; and

recording medium loading means where the recording medium is set, wherein

the second content decryption means, the encryption means, the recording means, the PC connecting means, and the recording medium loading means are realized by a piece of hardware,

the second content decryption means obtains the second content in the data that has been obtained by the obtaining means via the PC connecting means and decrypts the obtained second content, and

the recording means records the second content on the recording medium that has been set in the recording medium loading means.

7. The production protection system according to Claim 2, wherein

the data that is to be obtained by the obtaining means includes control information, which has been encrypted, for controlling operations on each content included in the obtained data, and

at least one of the first content decryption means and the second content decryption means includes a control information decryption unit for decrypting the control information.

8. The production protection system according to Claim 7, wherein

the second content decryption means includes the control information decryption unit, and

the personal computer that realizes the second content decryption means further executes software for decrypting the control information.

9. The production protection system according to Claim 8, wherein

the control information includes a key used for decrypting the second content,

the control information decryption unit further includes a first authentification encryption unit, and

the second content decryption means further includes a second authentification encryption unit, wherein

the first authentification encryption unit performs authentification of the second authentification encryption unit, performs encryption communication with the second authentification encryption unit, and transmits the key in the control information that has been decrypted by the control information decryption unit to the second authentification encryption unit when the authentification is successfully performed,

the second authentification encryption unit performs authentification of the first authentification encryption unit, performs encryption communication with the first authentification encryption unit, and obtains the key, and

the second content decryption means decrypts the second content using the key that the second authentification encryption unit has obtained.

10. The production protection system according to Claim 1, wherein

the obtaining means and the first content decryption means are realized by an apparatus that executes software for decrypting contents, and

the second content decryption means is realized by one of tamperproof hardware and an apparatus that executes tamperproof software.

11. The production protection system according to Claim 10, wherein

the obtaining means obtains the data by receiving the data from an outside network, and

the first content and the second content are same production that is expressed by digital data in different styles.

12. The production protection system according to Claim 11, further comprising:

encryption means for performing third encryption, which is different from the second encryption, on the second content that has been decrypted by the second content decryption means; and

recording means for recording at least part of the second content on which the third encryption has been performed by the encryption means on a recording medium.

13. The production protection system according to Claim 12, wherein the encryption means and a data communication channel between the second content decryption means and the encryption means are realized by one of tamperproof hardware and an apparatus that executes tamperproof software.

14. The production protection system according to

Claim 12, wherein

the first content is a music content for trial, and

the second content is a music content for sale and has a higher audio quality than the first content.

15. The production protection system according to Claim 14, further comprising replay means for replaying the first content that has been decrypted by the first content decryption means.

16. The production protection system according to Claim 12, wherein an encryption algorithm that is used by the second content decryption means partially differs from an encryption algorithm that is used for encryption by the encryption means.

17. The production protection system according to Claim 12, wherein

the encryption means includes:

a master key storage unit for storing a master key in advance;

a disk key creation unit for creating a disk key;

a disk key encryption unit for encrypting the disk key that has been created by the disk key creation unit using the master key;

a title key creation unit for creating a title key;

a title key encryption unit for encrypting the title key that has been created by the title key creation unit using the disk key; and

a content encryption unit for encrypting at least part of the second content that has been decrypted by the second content decryption means using the title key, and

the recording means records the disk key that has been encrypted by the disk key encryption unit, the title key that has been encrypted by the title key encryption unit, and the second content that has been encrypted by the content encryption unit on the recording medium.

18. The production protection system according to Claim 17, wherein

inherent information that is inherent in the recording medium is recorded on the recording medium in advance, and

the disk key creation unit creates the disk key according to the inherent information on the recording medium.

19. The production protection system according to Claim 17, wherein the title key creation unit creates the title key according to information, which is part of the

second content that has been decrypted by the second content decryption means.

20. The production protection system according to Claim 12, wherein

an inherent disk key inherent in the recording medium that has been encrypted using a master key is recorded on the recording medium in advance,

the encryption means includes:

a master key storage unit for storing the master key in advance;

a disk key creation unit for creating a disk key by decrypting the inherent disk key on the recording medium using the master key;

a title key creation unit for creating a title key;

a title key encryption unit for encrypting the title key that has been created by the title key creation unit using the disk key; and

a content encryption unit for encrypting at least part of the second content that has been decrypted by the second content decryption means using the title key, and

the recording means records the title key that has been encrypted by the title key encryption unit and the second content that has been encrypted by the content encryption unit on the recording medium.

21. The production protection system according to Claim 12, wherein

the recording medium includes a recording apparatus authentification unit for transmitting authentification information, and

the recording means judges correctness of the recording medium according to the authentification information that has been transmitted from the recording apparatus authentification unit, and performs the recording, in which at least part of the second content on which the third encryption has been performed is recorded on a recording medium, only when the recording medium is correct.

22. The production protection system according to Claim 10, further comprising:

encryption means for performing third encryption, which is different from the second encryption, on the second content that has been decrypted by the second content decryption means; and

recording means for recording at least part of the second content on which the third encryption has been performed by the encryption means on a recording medium.

23. The production protection system according to Claim 22, wherein an encryption algorithm that is used by

the second content decryption means partially differs from an encryption algorithm that is used for encryption by the encryption means.

24. The production protection system according to Claim 10, wherein

the data that is to be obtained by the obtaining means includes first content charging information, which is charging information on decryption of the first content when the data to be obtained includes the first content, and the data that is to be obtained includes second content charging information, which is charging information on decryption of the second content when the data to be obtained includes the second content,

the first content decryption means performs a charging operation according to the first content charging information when the first content is decrypted, and

the second content decryption means performs the charging operation according to the second content charging information when the second content is decrypted.

25. The production protection system according to Claim 1, wherein

the first encryption is performed using a first key,

the second encryption is performed using a second

key, which has a larger data size than the first key,

the data that is to be obtained by the obtaining means further includes control information, which has the first and second keys, for controlling operations on each content included in the data to be obtained,

the first content decryption means decrypts the first content using the first key, and

the second content decryption means decrypts the second content using the second key.

26. The production protection system according to Claim 25, wherein

the control information is encrypted using a control key that has been derived from a third key and a system common key, and included in the data that is to be obtained by the obtaining means,

the third key is encrypted using a fourth key and included in the data that is to be obtained,

the first content decryption means includes a first control information decryption unit for storing the system common key and a fifth key corresponding to the fourth key in advance, decrypting the third key using the fifth key, deriving the control key from the decrypted third key and the system common key, and decrypting the control information using the control key, and

the second content decryption means includes a

second control information decryption unit for storing the system common key and the fifth key corresponding to the fourth key in advance, decrypting the third key using the fifth key, deriving the control key from the decrypted third key and the system common key, and decrypting the control information using the control key.

27. A production protection system that deals with music contents for trial, on which first encryption has been performed, and music contents for sale, on which second encryption has been performed, a music content for sale is same music as a music content for trial and has a higher audio quality than the music content for trial,

the production protection system, comprising:

obtaining means for obtaining data that is a combination of a music content for trial and a music content for sale from an outside network;

first content decryption means for decrypting a first content in the data that has been obtained by the obtaining means using a first decryption method;

replay means for replaying a music of the first content that has been decrypted by the first content decryption means;

second content decryption means for decrypting a second content in the data that has been obtained by the obtaining means using a second decryption method, which is

more complicated than the first decryption method;

encryption means for performing third encryption, which is different from the second encryption, on the second content that has been decrypted by the second content decryption means; and

recording means for recording at least part of the second content on which the third encryption has been performed by the encryption means on a recording medium, wherein

the obtaining means and the first content decryption means are realized by a personal computer that executes software for decrypting contents, and

the second content decryption means, the encryption means, and a data communication channel between the second content decryption means and the encryption means are realized by one of tamperproof hardware and an apparatus that executes tamperproof software.

28. The production protection system according to Claim 27, wherein an encryption algorithm that is used by the second content decryption means partially differs from an encryption algorithm that is used for encryption by the encryption means.

29. (New) A production protection system dealing with contents that are digital production, comprising:

obtaining means for obtaining data including a first content, on which first encryption has been performed and a second content, on which second encryption has been performed, the second encryption is more difficult to break than the first encryption;

first content decryption means for decrypting the first content using a first decryption method that corresponds to the first encryption when the data that has been obtained by the obtaining means includes the first content; and

second content decryption means for decrypting the second content using a second decryption method that corresponds to the second encryption and is more difficult than the first decryption method when the data that has been obtained by the obtaining means includes the second content.

30. (New) The production protection system according to Claim 29, wherein

the first encryption is performed using a first key,

the second encryption is performed using a second key, which has a larger data size than the first key,

the data that is to be obtained by the obtaining means further includes control information, which has the first and second keys, for controlling operations on each content included in the data to be obtained,

the first content decryption means decrypts the first content using the first key, and

the second content decryption means decrypts the second content using the second key.

31. (New) The production protection system according to Claim 30,

wherein the control information is encrypted using a control key that has been derived from a third key and a system common key, and included in the data that is to be obtained by the obtaining means,

the third key is encrypted using a fourth key and included in the data that is to be obtained,

the first content decryption means includes a first control information decryption unit for storing the system common key and a fifth key corresponding to the fourth key in advance, decrypting the third key using the fifth key, deriving the control key from the decrypted third key and the system common key, and decrypting the control information using the control key, and

the second content decryption means includes a second control information decryption unit for storing the system common key and the fifth key corresponding to the fourth key in advance, decrypting the third key using the fifth key, deriving the control key from the decrypted third key and the system common key, and decrypting the control information using the control key.

32. (New) The production protection system according to Claim 29, wherein each of the first content and the second content is multimedia data that is digital production, and

the first content represents the same information as the second content but at a lower reproduction quality level.